

Concurrency Models with Causality and Events as Psi-calculi

Håkon Normann

IT University of Copenhagen,

{haakno,cristi}@ifi.uio.no

Cristian Prisacariu *

Dept. of Informatics, University of Oslo

Thomas Hildebrandt

IT University of Copenhagen, – Rued Langgaardsvej 7, 2300 Copenhagen, Denmark

hilde@itu.dk

Psi-calculi are a parametric framework for nominal calculi, where standard calculi are found as instances, like the pi-calculus, or the cryptographic spi-calculus and applied-pi. Psi-calculi have an interleaving operational semantics, with a strong foundation on the theory of nominal sets and process algebras. Much of the expressive power of psi-calculi comes from their logical part, i.e., assertions, conditions, and entailment, which are left quite open thus accommodating a wide range of logics. We are interested in how this expressiveness can deal with event-based models of concurrency. We thus take the popular prime event structures model and give an encoding into an instance of psi-calculi. We also take the recent and expressive model of Dynamic Condition Response Graphs (in which event structures are strictly included) and give an encoding into another corresponding instance of psi-calculi. The encodings that we achieve look rather natural and intuitive. Additional results about these encodings give us more confidence in their correctness.

1 Introduction

Psi-calculi [3] are a recent framework where various existing calculi can be found as instances. In particular, the spi- and applied-pi calculi [2, 1] are two instances of interest for security. Psi-calculi can also accommodate probabilistic models, by going through CC-pi [4, 6] which has already been treated as a corresponding psi-calculus instance. The theory of psi-calculi is based on nominal data structures [19]. Typed psi-calculus exists [13] as well as related instantiations as distributed pi-calculus [14]. Psi-calculi can be seen as a generalization of pi-calculus with two main features: (i) nominal data structures (i.e., general, possibly open, terms) in place of communication channels and also in place of the communicated data; and (ii) a rather open logic for capturing dependencies (i.e., through conditions and entailment) on the environment (i.e., assertions) of the processes.

The semantics of psi-calculi is given through structural operational rules and adopts an interleaving approach to concurrency, in the usual style of process algebras. On the other hand, event-based models of concurrency take a non-interleaving view. These usually form domains and are used to give denotational semantics, as e.g., done by Winskel in [24, 26]. Many times non-interleaving models of concurrency can actually distinguish between interleaving and, so called, “true” concurrency, as is the case with higher dimensional automata [20, 22, 7], configuration structures [9], or Chu spaces [10, 21]. The recent Dynamic Condition Response graphs (abbreviated DCR-graphs or DCRs) [11] is a model of concurrency with high expressive power which strictly extends event structures by refining the notions of dependent and conflicting events, and including the notion of response. Due to their graphical nature, DCRs have been successfully used in industry to model business processes [23].

*This author was partially supported by the project OffPAD with number E!8324 part of the Eurostars program funded by the EUREKA and European Community.

In this paper we are interested in how psi-calculi could accommodate the event structures model of concurrency [17, 25], with a final goal of capturing the DCRs model [11]. Event names in event-based models of concurrency are unique, and can thus be thought of nominals, whereas the execution of an event can be seen as a communication or action of some sort. The dependencies between events that an event structure defines can be captured with rather simple assertions on nominal data structures, whereas the notion of computation is captured through reduction steps between psi-processes. To be confident on the encodings, we like to see a correlation between the notions of concurrency from the two encoded models and the interleaving diamonds from the psi-calculus behaviour.

These are the basic ideas we follow in this work to give encodings of event structures and DCRs into corresponding instances of psi-calculus. After a couple of results meant to explain better the correlation between the encoding and the event structure model, we give a result that shows that the concurrency embodied by the event structure is captured in the encoding psi-process through the standard interleaving diamond. For the event structures encoding we also give a result that identifies the syntactic shape of those psi-processes which correspond exactly to event structures. Another feature of true concurrency models is that they are well behaved wrt. action refinement [8]. For this we give a result showing that action refinement is preserved by our translation; under a properly defined refining operation on psi-processes, which we define similarly to the refinement operation on the event structures.

2 Background

2.1 On psi-calculi

Psi-calculus [3] has been developed as a framework for defining nominal process calculi, like the many variants of the pi-calculus [16]. The psi-calculi framework is based on nominal datatypes, [3, Sec.2.1] giving an introduction to nominal sets used in psi-calculi. We will not explain much the nominal datatypes in this paper, but refer the reader to the book [19] which contains a thorough treatment of both the theory behind nominal sets as well as various applications (e.g., see [19, Ch.8] for nominal algebraic datatypes). We expect, though, some familiarity with notions of algebraic datatypes and term algebras.

The psi-calculi framework is parametric; instantiating the parameters accordingly, one obtains an *instance of psi-calculi*, like the pi-calculus, or the cryptographic spi-calculus. These parameters are:

T	terms (data/channels)
C	conditions
A	assertions

which are nominal datatypes not necessarily disjoint; together with the following operators:

$\leftrightarrow : \mathbf{T} \times \mathbf{T} \rightarrow \mathbf{C}$	channel equality
$\otimes : \mathbf{A} \times \mathbf{A} \rightarrow \mathbf{A}$	composition of assertions
$\mathbf{1} \in \mathbf{A}$	minimal assertion
$\vdash \subseteq \mathbf{A} \times \mathbf{C}$	entailment relation

Intuitively, terms can be seen as generated from a signature, as in term algebras; the conditions and assertions can be like in first-order logic; the minimal assertion being top/true, entailment the one from first-order logic, and composition taken as conjunction. It is helpful to think of assertions and conditions as logical formulas, and the entailment relation as an entailment in logic; but allow the intuition to think of logics abstractly, not just FOL, so that assertions and conditions are used to express any logical statements, where the entailment defines when assertions entail conditions (do not restrict to only thinking of

truth tables; e.g., in our encodings we will use an extended logic for sets, with membership, pairs, etc.). We will shortly exemplify how pi-calculus is instantiated in this framework. The operators are usually written infix, i.e.: $M \leftrightarrow N$, $\Psi \otimes \Psi'$, $\Psi \vdash \varphi$.

The above operators need to obey some natural requirements, when instantiated. Channel equality must be symmetric and transitive. The composition of assertions must be associative, commutative, and have $\mathbf{1}$ as unit; moreover, composition must preserve equality of assertions, where two assertions are considered equal iff they entail the same conditions (i.e., for $\Psi, \Psi' \in \mathbf{A}$ we define the equality $\Psi \simeq \Psi'$ iff $\forall \varphi \in \mathbf{C} : \Psi \vdash \varphi \Leftrightarrow \Psi' \vdash \varphi$).

The intuition is that assertions will be used to assert about the environment of the processes. Conditions will be used as guards for guarded (non-deterministic) choices, and are to be tested against the assertion of the environment for entailment. Terms are used to represent complex data communicated through channels, but will also be used to define the channels themselves, which can thus be more than just mere names, as in pi-calculus. The composition of assertions should capture the notion of combining assumptions from several components of the environment.

The syntax for building psi-process is the following (psi-processes are denoted by the P, Q, \dots ; terms from \mathbf{T} by M, N, \dots):

$\mathbf{0}$	Empty/trivial process
$\overline{M}\langle N \rangle.P$	Output
$\underline{M}\langle (\lambda \tilde{x})N \rangle.P$	Input
case $\varphi_1 : P_1, \dots, \varphi_n : P_n$	Conditional (non-deterministic) choice
$(\nu a)P$	Restriction of name a inside processes P
$P \mid Q$	Parallel composition
$!P$	Replication
$\langle \Psi \rangle$	Assertions

The input and output processes are as in pi-calculus only that the channel objects M can be arbitrary terms. In the input process the object $(\lambda \tilde{x})N$ is a pattern with the variables \tilde{x} bound in N as well as in the continuation process P . Intuitively, any term message received on M must match the pattern N for some substitution of the variables \tilde{x} . The same substitution is used to substitute these variables in P after a successful match. The traditional pi-calculus input $a(x).P$ would be modelled in psi-calculi as $\underline{a}\langle (\lambda x)x \rangle.P$, where the simple names a are the only terms allowed. Restriction, parallel, and replication are the standard constructs of pi-calculus.

The case process behaves like one of the P_i for which the condition φ_i is entailed by the current environment assumption, as defined by the notion of *frame* which we present later. This notion of frame is familiar from the applied pi-calculus, where it was introduced with the purpose of capturing static information about the environment (or seen in reverse, the frame is the static information that the current process exposes to the environment). A particular use of case is as **case** $\varphi : P$ which can be read as **if** φ **then** P . Another special usage of case is as **case** $\top : P_1, \top : P_2$, where $\Psi \vdash \top$ is a special condition that is entailed by any assertion, like $a \leftrightarrow a$; this use is mimicking the pi-calculus non-deterministic choice $P_1 + P_2$. Infinite summation is sometimes found in process algebras, e.g., in Milner's SCCS [15]. In the case of psi-calculi an infinite case construct can be used as **case** $\tilde{\varphi}_i : \tilde{P}_i$ where we use infinite lists to represent the respective condition/process pairs. There is no change to the semantics. The same semantics works for infinite parallel processes as well; though the replication is the preferred way to obtain infinite parallel components.

Assertions $\langle \Psi \rangle$ can float freely in a process (i.e., be put in parallel) describing assumptions about the environment. Otherwise, assertions can appear at the end of a sequence of input/output actions,

i.e., these are the guarantees that a process provides after it makes an action (on the same lines as in assume/guarantee reasoning about programs). Assertion processes are somehow similar to the active substitutions of the applied pi-calculus, only that assertions do not have computational behaviour, but only restrict the behaviour of the other constructs by providing their assumptions about the environment.

Example 2.1 (pi-calculus as an instance) *To obtain pi-calculus [16] as an instance of psi-calculus use the following, built over a single set of names \mathcal{N} :*

$$\begin{aligned} \mathbf{T} &\triangleq \mathcal{N} \\ \mathbf{C} &\triangleq \{a = b \mid a, b \in \mathbf{T}\} \\ \mathbf{A} &\triangleq \{\mathbf{1}\} \\ \leftrightarrow &\triangleq = \\ \vdash &\triangleq \{(\mathbf{1}, a = a) \mid a \in \mathbf{T}\} \end{aligned}$$

with the trivial definition for the composition operation. The only terms are the channel names $a \in \mathcal{N}$, and there is no other assertion than the unit. The conditions are equality tests for channel names, where the only successful tests are those where the names are equal. Hence, channel comparison is defined as just name equality.

Psi-calculus is given an operational semantics in [3] using labelled transition systems, where the nodes are the process terms and the transitions represent one reduction step, labelled with the action that the process executes. The actions, generally denoted by α, β , represent respectively the input and output constructions, as well as τ the internal synchronization/communication action:

$$\overline{M}\langle (v\tilde{a})N \rangle \mid \underline{M}\langle N \rangle \mid \tau$$

Transitions are done in a context, which is represented as an assertion Ψ , capturing assumptions about the environment:

$$\Psi \triangleright P \xrightarrow{\alpha} P'$$

Intuitively, the above transition could be read as: The process P can perform an action α in an environment respecting the assumptions in Ψ , after which it would behave like the process P' .

The context assertion is obtained using the notion of *frame* which essentially collects (using the composition operation) the outer-most assertions of a process. The frame $\mathcal{F}(P)$ is defined inductively on the structure of the process as:

$$\begin{aligned} \mathcal{F}(\langle \Psi \rangle) &= \Psi \\ \mathcal{F}(P \mid Q) &= \mathcal{F}(P) \otimes \mathcal{F}(Q) \\ \mathcal{F}((va)P) &= (va).\mathcal{F}(P) \\ \mathcal{F}(!P) &= \mathcal{F}(\text{case } \tilde{\phi} : \tilde{P}) = \mathcal{F}(\overline{M}\langle N \rangle.P) = \mathcal{F}(\underline{M}\langle (\lambda \tilde{x})N \rangle.P) = \mathbf{1} \end{aligned}$$

Any assertion that occurs under an action prefix or a condition is not visible in the frame.

We give only an exemplification of the transition rules for psi-calculus, and refer to [3, Table 1] for the full definition. The (CASE) rule shows how the conditions are tested against the context assertions. The communication rule (COM) shows how the environment processes executing in parallel contribute their top-most assertions to make the new context assertion for the input-output action of the other parallel processes. In the (COM) rule the assertions Ψ_P and Ψ_Q come from the frames of $\mathcal{F}(P) = (v\tilde{b}_P)\Psi_P$ respectively $\mathcal{F}(Q) = (v\tilde{b}_Q)\Psi_Q$. In (PAR) $bn(\alpha)\#Q$ says that the bound names of α are fresh in Q .

$$\frac{\Psi \vdash M \leftrightarrow K}{\Psi \triangleright \underline{M}\langle (\lambda \tilde{y})N \rangle.P \xrightarrow{\underline{K}N[\tilde{y}:=\tilde{L}]} P[\tilde{y}:=\tilde{L}]} \text{ (INN)} \quad \frac{\Psi \vdash M \leftrightarrow K}{\Psi \triangleright \overline{M}\langle N \rangle.P \xrightarrow{\overline{K}N} P} \text{ (OUT)}$$

$$\begin{array}{c}
\frac{\Psi \triangleright P_i \xrightarrow{\alpha} P' \quad \Psi \vdash \phi_i}{\Psi \triangleright \text{case } \tilde{\phi} : \tilde{P} \xrightarrow{\alpha} P'} \text{ (CASE)} \quad \frac{\Psi \otimes \Psi_Q \triangleright P \xrightarrow{\alpha} P' \quad bn(\alpha)\#Q}{\Psi \triangleright P|Q \xrightarrow{\alpha} P'|Q} \text{ (PAR)} \quad \frac{\Psi \triangleright P|!P \xrightarrow{\alpha} P'}{\Psi \triangleright !P \xrightarrow{\alpha} P'} \text{ (REP)} \\
\\
\frac{\Psi_Q \otimes \Psi \triangleright P \xrightarrow{\overline{M}(\tilde{v}\tilde{a})N} P' \quad \Psi_P \otimes \Psi \triangleright Q \xrightarrow{KN} Q' \quad \Psi_Q \otimes \Psi_P \otimes \Psi \vdash M \leftrightarrow K}{\Psi \triangleright P|Q \xrightarrow{\tau} (\tilde{v}\tilde{a})(P'|Q')} \text{ (COM)}
\end{array}$$

There is no transition rule for the assertion process; this is only used in constructing frames. Once an assertion process is reached, the computation stops, and this assertion remains floating among the other parallel processes and will be composed part of the frames, when necessary, like in the case of the communication rule. The empty process has the same behaviour as, and thus can be modelled by, the trivial assertion $(\mathbf{1})$.

2.2 On event structures

For event structures we try to follow the standard notation and terminology from [26, sec.8].

Definition 2.2 (prime event structures) A labelled prime event structure *over alphabet Act* is a tuple $\mathcal{E} = (E, \leq, \#, l)$ where E is a possibly infinite set of events, $\leq \subseteq E \times E$ is a partial order (the causality relation) satisfying

1. the principle of finite causes, i.e.: $\forall e \in E : \{d \in E \mid d \leq e\}$ is finite,
 - and $\# \subseteq E \times E$ is an irreflexive, symmetric binary relation (the conflict relation) satisfying
 2. the principle of conflict heredity, i.e., $\forall d, e, f \in E : d \leq e \wedge d \# f \Rightarrow e \# f$.
- and $l : E \rightarrow \text{Act}$ is the labelling function. Denote by \mathbf{E} the set of all prime event structures.

Intuitively, a prime event structure models a concurrent system by taking $d \leq e$ to mean that event d is a prerequisite of event e , i.e., event e cannot happen before event d has been done. A conflict $d \# e$ says that events d and e cannot both happen in the same run.

Definition 2.3 (concurrency) Casual independence (concurrency) *between events* is defined in terms of the above two relations as

$$d \parallel e \triangleq \neg(d \leq e \vee e \leq d \vee d \# e)$$

capturing the intuition that two events are concurrent when there is no causal dependence between the two and they are not in conflict.

The behaviour of an event structure is described by subsets of events that happened in some (partial) run. This is called a *configuration* of the event structure, and *steps* can be defined between configurations.

Definition 2.4 (configurations) Define a configuration of an event structure $\mathcal{E} = (E, \leq, \#)$ to be a finite subset of events $C \subseteq E$ that respects:

1. conflict-freeness: $\forall e, e' \in C : \neg(e \# e')$ and,
2. downwards-closure: $\forall e, e' \in E : e' \leq e \wedge e \in C \Rightarrow e' \in C$.

We denote the set of all configurations of some event structure by $\mathcal{C}_{\mathcal{E}}$.

Note in particular that \emptyset is a configuration (i.e., the root configuration) and that any set $[e] \triangleq \{e' \in E \mid e' \leq e\}$ is also a configuration determined by the single event e . Events determine steps between configurations in the sense that $C \xrightarrow{e} C'$ whenever C, C' are configurations, $e \notin C$, and $C' = C \cup \{e\}$.

Remark 2.5 *It is known (see e.g., [26, Prop.18]) that prime event structures are fully determined by their sets of configurations, i.e., the relations of causality, conflict, and concurrency can be recovered only from the set of configurations $\mathcal{C}_\mathcal{E}$ as follows:*

1. $e \leq e'$ iff $\forall C \in \mathcal{C}_\mathcal{E} : e' \in C \Rightarrow e \in C$;
2. $e \sharp e'$ iff $\forall C \in \mathcal{C}_\mathcal{E} : \neg(e \in C \wedge e' \in C)$;
3. $e \parallel e'$ iff $\exists C, C' \in \mathcal{C}_\mathcal{E} : e \in C \wedge e' \notin C \wedge e' \in C' \wedge e \notin C' \wedge C \cup C' \in \mathcal{C}_\mathcal{E}$.

For some event e we denote by $\leq e = \{e' \in E \mid e' \leq e\}$ the set of all events which are conditions of e (which is the same as the notation $\lceil e \rceil$ from [26], but we prefer to use the above so to be more in sync with similar notations we use in this paper for similar sets defined for DCRs too), and $\sharp e = \{e' \in E \mid e' \sharp e\}$ those events in conflict with e .

2.3 On DCR-graphs

Dynamic Condition Response graphs (DCR-graphs) is a recent model of concurrency, which generalizes event structures by taking into account progress in terms of demanded responses, while giving a finite model of possibly infinite behaviour. Using a graphic notation along with the formal, it is already used in industry for workflow management. We follow the notations for DCRs from [11, 12].

Definition 2.6 (DCR Graphs) *We define a Dynamic Condition Response Graph to be a tuple $G = (E, M, \rightarrow\bullet, \bullet\rightarrow, \rightarrow\bowtie, \rightarrow+, \rightarrow\%, L, l)$ where*

1. E is a set of events,
2. $M \in 2^E \times 2^E \times 2^E$ is the initial marking,
3. $\rightarrow\bullet, \bullet\rightarrow, \rightarrow\bowtie, \rightarrow+, \rightarrow\% \subseteq E \times E$ are respectively called the condition, response, milestone, include, and exclude relations,
4. $l : E \rightarrow L$ is a labelling function mapping events to labels from L .

For any relation $\rightarrow \in \{\rightarrow\bullet, \bullet\rightarrow, \rightarrow\bowtie, \rightarrow+, \rightarrow\%\}$, we use the notation $e \rightarrow$ for the set $\{e' \in E \mid e \rightarrow e'\}$ and $\rightarrow e$ for the set $\{e' \in E \mid e' \rightarrow e\}$ of events $e' \in E$ which are in the respective relation with e .

A marking $M = (Ex, Re, In)$ represents a state of the DCR. One should understand Ex as the set of *executed* events, Re the set of *response* events that must happen sometime in the future, and In the set of *included* events, i.e., those that *may* happen in the next steps. The five relations impose constraints on the events and dictate the dynamic inclusion and exclusion of events.

For a DCR graph $(E, M, \rightarrow\bullet, \bullet\rightarrow, \rightarrow\bowtie, \rightarrow+, \rightarrow\%)$ and a marking $M = (Ex, Re, In)$, we say that an *event* $e \in E$ is *enabled* in M , written $M \vdash e$, iff $e \in In \wedge (In \cap \rightarrow\bullet e) \subseteq Ex \wedge (In \cap \rightarrow\bowtie e) \subseteq E \setminus Re$. Intuitively, an event can only happen if it is included, all its included preconditions have been executed, and none of the included events that are milestones for it are scheduled responses. The behaviour of a DCR is given through transitions between markings done by executing enabled events. The result of the execution of the event e in marking $M = (Ex, Re, In)$ is defined as the new marking $M' \stackrel{def}{=} (Ex \cup \{e\}, (Re \setminus \{e\}) \cup e \bullet\rightarrow, (In \setminus e \rightarrow\%) \cup e \rightarrow+)$. We denote a transition as $M \xrightarrow{e} M'$. An event can happen an arbitrary number of times as long as it is enabled. Events that should happen only once must explicitly be excluded.

An event structure (E, \leq, \sharp, l) is a special case of a DCR graph $(E, M, \leq, \emptyset, \emptyset, \emptyset, \sharp \cup id)$ where each event is excluding itself, i.e., cannot be done multiple times, and the conflict relation is modelled by mutual exclusion. The response, include, and milestone relations are empty, and initially all events are included, as the marking $M = (\emptyset, \emptyset, E)$, i.e., all events can be executed; this comes from [11, Prop.1&3].

Essentially, the conflict relation excludes all related events; and the causality relation is the condition relation of the DCR. The rest of the DCR relations are just additions wrt. the event structures model, therefore should be empty. Moreover, the initial marking has no executed events and no responses, but all events are initially included. Opposed to the behaviour of event structures, in full DCRs we also have that the causality between events can change during the run, as events are included or excluded. Moreover, the conflict in DCRs is not permanent as is the case with event structures or with the various proposals of cancellation of Pratt. Conflict in DCR can be transient since an event can be included and excluded during a run. So, already at the conflict and causality relations, the DCRs depart from event structures in a non-trivial manner.

DCRs have peculiar aspects which offer them good expressive power that proved useful in various practical situations, like for business workflows. But we are not concerned with explaining or motivating these more, as the related literature does a much better job. We are concerned with finding a nice and intuitive encoding of DCRs in the expressive psi-calculi framework.

3 Encoding event structures in psi-calculi

Due to their popularity, we have chosen to encode, in this section, the version of event structures called *prime* as defined in Definition 2.2. These have many nice features like correlations with domains which makes them a good candidate for being used for denotational semantics of concurrent programs. Nevertheless, we believe that other, more general, versions of event structures, like those from [25] or [9], can be encoded in psi-calculi following similar ideas as we give here.

Definition 3.1 (event psi-calculus) *We define a psi-calculus instance, called eventPsi, parametrized by a nominal set E , to be understood as events, by providing the following definitions of the key elements of a psi-calculus instance:*

$$\begin{aligned} \mathbf{T} &\stackrel{\text{def}}{=} E & \mathbf{C} &\stackrel{\text{def}}{=} 2^E \times 2^E & \mathbf{A} &\stackrel{\text{def}}{=} 2^E & \hookleftrightarrow &\stackrel{\text{def}}{=} & \otimes &\stackrel{\text{def}}{=} \cup & \mathbf{1} &\stackrel{\text{def}}{=} \emptyset \\ \vdash &\stackrel{\text{def}}{=} \Psi \vdash \varphi \text{ iff } (\pi_L(\varphi) \subseteq \Psi) \wedge (\Psi \cap \pi_R(\varphi) = \emptyset) & \Psi &\vdash a \hookleftrightarrow b \text{ iff } a = b \end{aligned}$$

where \mathbf{T} , \mathbf{C} , and \mathbf{A} are nominal data types built over the nominal set E , and π_L, π_R are the standard left/right projection functions for pairs. Denote by $\text{en}(P) \subseteq E$ the event names appearing in a process P .

The conditions \mathbf{C} are pairs of subsets of events, which intuitively will hold the enabling conditions for an event, i.e., the left set holding those events it depends on and the right set holding those events it is in conflict with. The assertions \mathbf{A} intuitively can be understood as capturing the set of all executed events, i.e., a configuration of the event structure. Channel equivalence is equality of event names, as in standard pi-calculus. Composition of two assertions is the union of the sets. The entailment \vdash intuitively captures when events may fire, thus describing when events are enabled by a configuration.

It is easy to see that our definitions respect the restrictions of making a psi-calculus instance. In particular, channel equivalence is symmetric and transitive since equality is. The \otimes is compositional, associative and commutative, as \cup is; and moreover $\emptyset \cup S = S$, for any set S , i.e., $\mathbf{1}$ is the identity.

Definition 3.2 (event structures to eventPsi) *We define a function ESPSI which given an event structure $\mathcal{E} = (E, \leq, \#)$ and a configuration C of \mathcal{E} , returns an eventPsi-process $P_E = |_{e \in E} P_e$ with $P_e = (\{e\})$ if $e \in C$, otherwise $P_e = \text{case } \varphi_e : \bar{e}\langle e \rangle. (\{e\})$, where $\varphi_e = (\leq e, \#e)$.*

A process generated by the ESPSI function is built up from smaller “event processes” put in parallel. These come in two forms: those corresponding to the events in the configuration of the translated event structure (i.e., those that already happened), and processes corresponding to events that have not happened yet. For the latter we use a condition φ_e that contains the set $\leq e$ of events e is depending on and the set $\sharp e$ of events e is in conflict with. Together these two sets along with the frame of the entire psi-process, decide, through the entailment, if the event can execute or not. When an event happens we will have a transition over the channel with the same name as the event. Usually an event structure is encoded into eventPsi starting from the empty configuration, i.e., with no behaviour.

The set \mathbf{T} may be infinite, hence elements of \mathbf{A} and \mathbf{C} may be infinite terms (sets). In the encoding produced by ESPSI, the conditions have $\pi_L(\varphi)$ finite, because of the principle of finite causes of Definition 2.2.1 that event structures respect. Still, the $\pi_R(\varphi)$ may be infinite, because there is no restriction on the conflict relation in event structures, and thus an event can be in conflict with infinitely many events, therefore ESPSI may create infinite condition terms.

An intuitive example where this would appear is when we model looping behaviour of a system with event structures, and we have a looping branch, which would be unfolded into infinitely many sequential events, and we have a second branch which cancels this looping branch (i.e., as with a choice). The cancelling of the looping branch would mean cancelling all the infinitely many events that encode this branch. That is to say, the single event is in conflict with all the events on the looping branch.

Assertion terms from \mathbf{A} , produced by ESPSI, are always finite because they encode, cf. Lemma 3.3, configurations, which are finite sets. Therefore, it is not problematic to have the infinite part of the conditions, since the only place where this is used is in deciding the entailment, which would thus always terminate, hence be decidable for any assertion/configuration used in the encoding.

Besides this, the encoding ESPSI builds in parallel infinitely many processes, one for each $e \in E$. For practical reasons infinite terms are not desired. But there are works with infinite terms, like infinite summation in SCCS, infinite case construct for psi-calculus, or infinite conjunctions in some logics. Such infinite formulas usually make the presentation more nice. In our case we also wanted to have the nice presentation, therefore we opted to generate infinite terms. From our terms it is clear to see the correlation with the event structures. We work the same as in event structures, by tacitly having infinite events, thus infinite parallel processes. Encoding the infinite terms with the replication (i.e., one replication of an infinite case construct) would make the presentation more cluttered, with the details easily becoming unpleasant.

We could say that prime event structures are “wildly” infinite. If we would otherwise take a kind of event structures that are regular, i.e., are build from some operations like choice and sequence, and the infinity comes only from some recursion operation, then we think that this infinity could be encoded with the finite apparatus of psi-calculi. But it is not clear which event structures are “regular”; and for our purposes the prime event structures are a good enough concurrency model to look at.

Our intention is to investigate the expressive power of the psi-calculi framework; the power of its logical part, i.e., the assertions, conditions, and entailment, and the complex nominal data structures that can be used both for communication and for transmitted data.

Lemma 3.3 (correspondence configuration–frame) *For any event structure \mathcal{E} and configuration $C_{\mathcal{E}}$, the frame of the eventPsi-process $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ corresponds to the configuration $C_{\mathcal{E}}$.*

Proof: Denote $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) = P_E$ as in Definition 3.2. The frame of P_E is the composition with \otimes of the frames of P_e for $e \in E$. As P_e is either $(\llbracket \{e\} \rrbracket)$ if $e \in C_{\mathcal{E}}$ or **case** $\varphi_e : \bar{e}(e).(\llbracket \{e\} \rrbracket)$ then the frame of P_e would be either $\mathcal{F}(\llbracket \{e\} \rrbracket) = \{e\}$ or $\mathcal{F}(\text{case } \varphi_e : \bar{e}(e).(\llbracket \{e\} \rrbracket)) = \mathbf{1}$. Thus the frame of P_E is the \otimes of $\mathbf{1}$ ’s and all events in $C_{\mathcal{E}}$, thus having that the frame is the union of all events in $C_{\mathcal{E}}$ \square

Lemma 3.4 (transitions preserve configurations) *For some event structure \mathcal{E} and some configuration of it $C_{\mathcal{E}}$, any transition from this configuration $C_{\mathcal{E}} \xrightarrow{e} C'_{\mathcal{E}}$ is matched by a transition $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{\bar{e}e} \text{ESPSI}(\mathcal{E}, C'_{\mathcal{E}})$ in the corresponding eventPsi-process. The other way, any transition $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{\bar{e}e} P'$ is matched by a step $C_{\mathcal{E}} \xrightarrow{e} C'_{\mathcal{E}}$, with $P' = \text{ESPSI}(\mathcal{E}, C'_{\mathcal{E}})$.*

Proof: Before the event e is executed we have that our eventPsi-process $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ can be written in the form $P = \text{case } \varphi_e : \bar{e}\langle e \rangle. (\{e\}) \mid Q$. By Lemma 3.3 we know that the frame of P is the same as $C_{\mathcal{E}}$, i.e., we have that $\mathcal{F}(P) = \mathbf{1} \otimes \mathcal{F}(Q) = \Psi_Q = C_{\mathcal{E}}$ before e has happened, and $e \notin C_{\mathcal{E}}$.

We can observe the transition between eventPsi-processes by the following proof tree, using the transition rules of psi-calculi.

An event e can happen if the corresponding condition in the **case** construct is entailed by the appropriate assertion $\Psi_Q \vdash \varphi_e$. This forms the right condition of the (CASE) rule, saying that all the preconditions of e are met, and e is not in conflict with any event that has happened. This condition is met because $C_{\mathcal{E}} = \Psi_Q$ and the assumption of the lemma, i.e., the existence of the step, which implies that e is enabled by the configuration $C_{\mathcal{E}}$, meaning exactly what the definition of the entailment relation needs.

After $\bar{e}e$ has happened we have $P' = (\{e\}) \mid Q$ and $\mathcal{F}(P') = \mathcal{F}(\{e\}) \otimes \mathcal{F}(Q) = \{e\} \cup \Psi_Q$, meaning that the frame of P' corresponds to $C'_{\mathcal{E}} = C_{\mathcal{E}} \cup \{e\}$. From the definition of the translation function ESPSI it is easy to see that $\text{ESPSI}(\mathcal{E}, C'_{\mathcal{E}}) = (\{e\}) \mid Q$.

The second part of the lemma is especially easy after going through the proofs of the next results. \square

Theorem 3.5 (preserving concurrency) *For an event structure $\mathcal{E} = (E, \leq, \#)$ with two concurrent events $e \parallel e'$ then in the translation $\text{ESPSI}(\mathcal{E}, \emptyset)$ we find the behaviour forming the interleaving diamond, i.e., there exists $C_{\mathcal{E}}$ s.t. $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{e} P_1 \xrightarrow{e'} P_2$ and $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{e'} P_3 \xrightarrow{e} P_4$ with $P_2 = P_4$.*

Proof: In a prime event structure if two events e, e' are concurrent then there exists a configuration C reachable from the root which contains the conditions of both events, i.e., $\leq e \subseteq C$ and $\leq e' \subseteq C$, and does not contain any of the two events, i.e., $e, e' \notin C$ (cf. Remark 2.5). Take this configuration as the one $C_{\mathcal{E}}$ sought in the theorem. Therefore we have the following steps in the event structure: $C_{\mathcal{E}} \xrightarrow{e} C_{\mathcal{E}} \cup e$, $C_{\mathcal{E}} \xrightarrow{e'} C_{\mathcal{E}} \cup e'$, $C_{\mathcal{E}} \cup e \xrightarrow{e'} C_{\mathcal{E}} \cup \{e, e'\}$, and $C_{\mathcal{E}} \cup e' \xrightarrow{e} C_{\mathcal{E}} \cup \{e, e'\}$.

Since $C_{\mathcal{E}}$ is reachable from the root then by Lemma 3.4 all the steps are preserved in the behaviour of the eventPsi-process $\text{ESPSI}(\mathcal{E}, \emptyset)$, meaning that $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ is reachable from (i.e., part of the behaviour of) $\text{ESPSI}(\mathcal{E}, \emptyset)$.

Since $e, e' \notin C_{\mathcal{E}}$ we have that $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ is in the form $P_0 = P_e \mid P_{e'} \mid Q$ with P_e and $P_{e'}$ processes of kind **case**. From Lemma 3.3 we know that the frame of $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ is the assertion corresponding to $C_{\mathcal{E}}$, which is $\mathcal{F}(P_e \mid P_{e'} \mid Q) = \{\emptyset\} \cup \{\emptyset\} \cup \Psi_Q = \Psi_Q$.

From Lemma 3.4 we see the transitions between the eventPsi-processes: $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{e} P_1 \xrightarrow{e'} P_2$ with $P_2 = (\{e\}) \mid (\{e'\}) \mid Q$ as well as $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{e'} P_3 \xrightarrow{e} P_4$ with $P_4 = (\{e\}) \mid (\{e'\}) \mid Q$. We thus have the expected interleaving diamond.

As a side, remark that $\mathcal{F}(P_1) = \mathcal{F}(P_0) \otimes (\{e\})$ and $\mathcal{F}(P_3) = \mathcal{F}(P_0) \otimes (\{e'\})$ thus $\mathcal{F}(P_1) \otimes \mathcal{F}(P_3) = \mathcal{F}(P_0) \otimes (\{e\}) \otimes (\{e'\}) = \mathcal{F}(P_4)$, which says that $e \in \mathcal{F}(P_1) \wedge e' \notin \mathcal{F}(P_1) \wedge e' \in \mathcal{F}(P_3) \wedge e \notin \mathcal{F}(P_3) \wedge \mathcal{F}(P_1) \otimes \mathcal{F}(P_3) = \mathcal{F}(P_4)$. Using Lemma 3.3 these can be correlated with configurations and thus we can see the definition of concurrency from configurations as in Remark 2.5.3. \square

The proof of Theorem 3.5 hints at an opposite result, stating a true concurrency rule for eventPsi-processes. Intuitively the next result says that any two events that in the behaviour of the eventPsi-process make up the interleaving diamond are concurrent in the corresponding event structure.

Theorem 3.6 (interleaving diamonds) *For any event structure \mathcal{E} , in the corresponding eventPsi-process $\text{ESPSI}(\mathcal{E}, \emptyset)$, for any interleaving diamond $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{e} P_1 \xrightarrow{e'} P_2$ and $\emptyset \triangleright \text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) \xrightarrow{e'} P_3 \xrightarrow{e} P_4$ with $P_2 = P_4$, for some configuration $C_{\mathcal{E}} \in \mathcal{C}_{\mathcal{E}}$, we have that the events $e || e'$ are concurrent in \mathcal{E} .*

Proof: Since $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ has two outgoing transitions labelled with the events e and e' it means that $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ is in the form $P_0 = P_e | P_{e'} | Q$ with P_e and $P_{e'}$ processes of kind **case**. From Lemma 3.3 we know that the frame of $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}})$ is the assertion corresponding to $C_{\mathcal{E}}$, which is $\mathcal{F}(P_e | P_{e'} | Q) = \{\emptyset\} \cup \{\emptyset\} \cup \Psi_Q = \Psi_Q$.

We thus have that $e, e' \notin \Psi_Q$ and $P_0 \xrightarrow{e} P_1$ and $P_0 \xrightarrow{e'} P_3$. This means that for these two transitions to be possible it must be that the precondition for e and e' respectably must be met. Since $e, e' \notin \Psi_Q$ it must be that $e' \notin \pi_L(\varphi_e)$ and $e \notin \pi_L(\varphi_{e'})$. Since $\pi_L(\varphi_e)$ is the same as the set $\leq e$ and $\pi_L(\varphi_{e'})$ the set $\leq e'$ we have the two parts of the Definition 2.3 that concern \leq for the casual independence (concurrency) of the events e, e' , i.e., $\neg(e' \leq e \vee e' \leq e)$. After the two transitions are taken we have that $P_1 = \langle e \rangle | P_{e'} | Q$ and $P_3 = P_e | \langle e' \rangle | Q$. We thus have that $e \in \mathcal{F}(P_1)$ and $e' \in \mathcal{F}(P_3)$. For the transition $P_1 \xrightarrow{e'} P_2$ to happen we must have that $e \notin \pi_R(\varphi_{e'})$ and for $P_3 \xrightarrow{e} P_4$ we must have $e' \notin \pi_R(\varphi_e)$. This is the same as $e' \notin \sharp e$ and $e \notin \sharp e'$ which makes the last part of Definition 2.3 concerning the conflict relation, i.e., $\neg(e' \sharp e)$. This completes the proof, showing $e || e'$. \square

We have seen that the eventPsi-processes that we obtain from event structures in Definition 3.2 have a specific syntactic form. But the eventPsi instance allows any process term to be constructed over the three nominal data-types that we gave in Definition 3.1. The question is which of all these eventPsi-processes correspond exactly to event structures? We want to have syntactic restrictions on how to write eventPsi-process terms so that we are sure that there exists an event structure corresponding to each such restricted process term.

Theorem 3.7 (syntactic restrictions) *Consider eventPsi-process terms built only with the following grammar:*

$$P_{ES} := \langle e \rangle \mid \text{case } \varphi : \bar{e}\langle e \rangle . \langle e \rangle \mid P_{ES} | P_{ES}$$

*Moreover, a term P_{ES} has to respect the following constraints, for any $\varphi_e, \varphi_{e'}$ from **case** $\varphi_e : \bar{e}\langle e \rangle . \langle e \rangle$ respectively **case** $\varphi_{e'} : \bar{e'}\langle e' \rangle . \langle e' \rangle$:*

1. *conflict:* $e \notin \pi_R(\varphi_e)$ and $e' \in \pi_R(\varphi_e)$ iff $e \in \pi_R(\varphi_{e'})$;
2. *causality:* $e \notin \pi_L(\varphi_e)$ and if $e \in \pi_L(\varphi_{e'})$ then $e' \notin \pi_L(\varphi_e) \wedge \pi_L(\varphi_e) \subset \pi_L(\varphi_{e'})$;
3. *executed events:* P_{ES} cannot have both $\langle e \rangle$ and **case** $\varphi : \bar{e}\langle e \rangle . \langle e \rangle$ for any e , nor multiples of each.

For any such restricted process P_{ES} there exists an event structure \mathcal{E} and configuration $C_{\mathcal{E}} \in \mathcal{C}_{\mathcal{E}}$ s.t.

$$\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) = P_{ES}.$$

Proof: From a eventPsi-process P_{ES} defined as in the statement of the theorem, we show how to construct an event structure $\mathcal{E} = (E, \leq, \sharp)$ and a configuration $C_{\mathcal{E}}$. We have that P_{ES} is built up of assertion processes and case guarded outputs, i.e., $P_{ES} = (\mid_{e \in E_c} \langle e \rangle) \mid (\mid_{f \in E_r} \text{case } \varphi_f : \bar{f}\langle f \rangle . \langle f \rangle)$.

Because of the third restriction on P_{ES} we know that E_c and E_r are sets, as no multiples of the same process can exist. Moreover, these two sets are disjoint. For otherwise, assume we have $\langle e \rangle \mid \text{case } \varphi_e : \bar{e}\langle e \rangle . \langle e \rangle$ part of P_{ES} . This is the same as if e has happened already and e may happen in future, which cannot be the case for event structures.

We take $C_{\mathcal{E}}$ to be the frame of $\mathcal{F}(P_{ES}) = E_c$. We take the set of events to be $E = E_c \cup E_r$. We construct the causality and conflict relations from the processes in the second part of P_{ES} as follows:

$\leq = \cup_{e \in E_r} \{(e', e) \mid e' \in \pi_L(\varphi_e)\}$ and $\sharp = \cup_{e \in E_r} \{(e', e) \mid e' \in \pi_R(\varphi_e)\}$. We prove that the causality relation is a partial order. For irreflexivity just use the first part of the second restriction on P_{ES} . For antisymmetry assume that $e \leq e' \wedge e' \leq e \wedge e \neq e'$ which is the same as having $e \in \pi_L(\varphi_{e'}) \wedge e' \in \pi_L(\varphi_e)$. This contradicts the second restriction on P_{ES} . Transitivity is easy to obtain from the second restriction which says that when $e \leq e'$ then all the conditions of e are a subset of the conditions of e' . We prove that the conflict relation is irreflexive and symmetric. The irreflexivity follows from the first part of the first restriction on P_{ES} , whereas the symmetry is given by the second part.

It is easy to see that for the constructed event structure and the configuration chosen above, we have $\text{ESPSI}(\mathcal{E}, C_{\mathcal{E}}) = P_{ES}$. The encoding function ESPSI takes all events from $C_{\mathcal{E}}$ to the left part of the P_{ES} , whereas the remaining events, i.e., from E_r are taken to **case** processes where for each event $f \in E_r$ the corresponding condition φ_f contains the causing events respectively the conflicting events. But these correspond to how we built the two relations above. \square

3.1 Refinement

We want to be able to refine psi processes on the same line as labelled event structures are refined in [8]. We recall below the definition of refinement of event structures from [8].

A *refinement function* ref , is a function from actions to event structures without conflict (i.e., the conflict relation is empty). This is considered as a given function to be used in the *refinement operation*. This refinement operation can be also seen as a function from event structures together with functions as above, and returning new event structures, i.e., like an algorithm. For notation economy this algorithm is also denoted by ref , to connect it with the essential input it takes as the refinement function $\text{ref} : \text{Act} \rightarrow \mathbf{E}_{\sharp}$ (with \mathbf{E}_{\sharp} denoting conflict-free prime event structures).

Definition 3.8 (refinement for prime event structures) *For an event structure \mathcal{E} with events labelled by $l : E \rightarrow \text{Act}$ with actions from Act we have the following definitions.*

(i) A Function $\text{ref} : \text{Act} \rightarrow \mathbf{E}_{\sharp}$ is called a *refinement function* (for prime event structures) iff $\forall a \in \text{Act} : \text{ref}(a)$ is a non-empty, finite and conflict-free labelled prime event structure.

(ii) Let $\mathcal{E} \in \mathbf{E}$ and let ref be a refinement function.

Then $\text{ref}(\mathcal{E})$ is the prime event structure defined by:

- $E_{\text{ref}(\mathcal{E})} := \{(e, e') \mid e \in E_{\mathcal{E}}, e' \in E_{\text{ref}(l_{\mathcal{E}}(e))}\}$, where $E_{\text{ref}(l_{\mathcal{E}}(e))}$ denotes the set of events of the event structure $\text{ref}(l_{\mathcal{E}}(e))$,
- $(d, d') \leq_{\text{ref}(\mathcal{E})} (e, e')$ iff $d \leq_{\mathcal{E}} e$ or $(d = e \wedge d' \leq_{\text{ref}(l_{\mathcal{E}}(d))} e')$,
- $(d, d') \sharp_{\text{ref}(\mathcal{E})} (e, e')$ iff $d \sharp_{\mathcal{E}} e$,
- $l_{\text{ref}(\mathcal{E})}(e, e') := l_{\text{ref}(l_{\mathcal{E}}(e))}(e')$.

The intuition of refinement is to take one action (which is thought as an abstraction) and give it more structure. Since the same action can be instantiated several times at different points in the system, i.e., by different events, all these events labelled by the same action are given more structure by replacing them with a new event structure. For example one event can become a sequence of events, or the parallel composition of deterministic components. But refinement is restricted to not contain conflicts, i.e., not contain choices. This is because of technical reasons that make it not possible to define the new conflict relation so to obtain prime event structures after refinement. But there are also natural counter-examples for requiring conflict-free refining event structures, and van Glabbeek and Goltz in [8] explain these much better than we ever could. We need a similar refinement operation for eventPsi-process terms.

Definition 3.9 Given a refinement function for event structures ref , we define an operation ref^Ψ that refines an eventPsi-process to a new one over the names

$$T^\Psi = \{(e, e') \mid e \in E, e' \in E_{ref(l(e))}\}.$$

An eventPsi-process P , build according to Theorem 3.7, with frame $\mathcal{F}(P) = \Psi_P$, is refined into a process

$$ref^\Psi(P) = |_{(e, e') \in T^P} P_{(e, e')}, \quad \text{with } T^P = \{(e, e') \mid e \in en(P), e' \in E_{ref(l(e))}\}$$

and $P_{(e, e')} = \langle \{(e, e')\} \rangle$, if $e \in \Psi_P$, otherwise $P_{(e, e')} = \mathbf{case} \ \varphi_{(e, e')} : \overline{(e, e')}(e, e'). \langle \{(e, e')\} \rangle$, with the conditions being

$$\varphi_{(e, e')} = (\leq(e, e'), \#(e, e')),$$

where $\leq(e, e') = \{(d, d') \mid d \in \pi_L(\varphi_e) \vee (d = e \wedge d' \in \leq_{ref(l(d))} e)\}$ and $\#(e, e') = \{(d, d') \mid d \in \pi_R(\varphi_e)\}$.

The new names are pairs of a parent event name (i.e., from the original process) and one of the event names from the refinement processes. We do not end up outside the eventPsi instance because we can rename any pair by names from E . Take any total order $<$ on E and define from it a total order $(e, e') < (d, d')$ iff $e < d \vee (e = d \wedge e' < d')$ on the pairs; rename any pair by an event from E while preserving the order, thus making T^Ψ the same as the \mathbf{T} of eventPsi.

We make new conditions for each of the new names (e, e') , where $\leq(e, e')$ contains all pairs of names s.t. either the left part is a condition for e , or the left part is the same as e but the right part is a condition for e' . The conflicts set $\#(e, e')$ contains all pairs of names with the first part a conflict for e . The refinement generates for each new pair one process which is either an assertion or a **case** process, depending on whether the first part of the event pair was in the frame of the old P or not.

Theorem 3.10 (refinement in eventPsi corresponds to refinement in ES) For any prime event structure \mathcal{E} we have that: $ESPSI(ref(\mathcal{E}), \emptyset) = ref^\Psi(ESPSI(\mathcal{E}, \emptyset))$.

Proof: As $\mathbf{T} = E$ and as T^Ψ is built from \mathbf{T} with the same rules as E_{ref} is built from E we have that $T^\Psi = E_{ref}$. Since the processes we work with are parallel compositions of assertion and **case** processes, it means we have to show that any assertion processes on the left is also found on the right of the equality (and vice versa), and the same for the **case** processes. Since we work with the empty initial configuration, then there are no assertion processes on neither sides.

The **case** processes on the left side are those generated by ESPSI from the pairs events returned by the ref from the event structure. This means that for each pair we have its condition built up as in the Definition 3.8. On the right side we have **case** processes for the original process before the refinement, with their respective conditions. But the ref^Ψ replaces these with many **case** processes, one for each new pair, and for each the conditions are build exactly as the ref is defining them. This says that we have the same number of **case** processes on both sides of the equality, and they have the same conditions. \square

4 DCR graphs as psi-calculi

We achieved a rather natural and intuitive translation of the prime event structures into an instance of psi-calculi. We made special use of the logic of psi-calculi, i.e., of the assertions and conditions and the entailment between these, as well as the assertion processes. Noteworthy is that we have not used the communication mechanism of psi-calculus, which is known to increase expressiveness.

We try to extend this approach from event structures to the DCRs. But it appears that we need the communication constructs on processes to keep track of the current marking of a DCR. The particularities and expressiveness of DCRs do not allow for a simple way of updating the marking, as was the case for event structures when just union with the newly executed event was enough. But once we use the communication, outputting a term representing the current marking, and incorporating an idea of generation (or age) of an assertion, where assertion composition keeps the newest generation which would be used for entailments, we get a nice natural encoding for DCRs in a psi-calculus instance. We can then see associations with the previous encoding of the event structures. The markings are kept in the assertions, i.e., as the frame of the process; the same as we did with the configurations of the event structures. Case processes are used for each event of the DCR, and the conditions of the case processes capture the information needed to decide when events of a DCR are enabled in a marking. The entailment relation then captures the enabling of events.

Definition 4.1 (dcrPsi instance) *We define an instantiation of Psi-calculi called dcrPsi by providing the following definitions:*

$$\mathbf{T} \stackrel{\text{def}}{=} \{m\} \cup \mathbf{A}$$

$$\mathbf{A} \stackrel{\text{def}}{=} 2^E \times 2^E \times 2^E \times \mathbb{N}$$

where E is a nominal set and \mathbb{N} is the nominal data structure capturing natural numbers using a successor function $s(\cdot)$ and generator 0 , whereas m is a single name used for communication;

$$\mathbf{C} \stackrel{\text{def}}{=} 2^E \times 2^E \times E \quad \leftrightarrow \stackrel{\text{def}}{=} \quad \mathbf{1} \stackrel{\text{def}}{=} (\emptyset, \emptyset, \emptyset, 0)$$

$$\llbracket (Ex, Re, In, G) \rrbracket \otimes \llbracket (Ex', Re', In', G') \rrbracket \stackrel{\text{def}}{=} \begin{cases} \llbracket (Ex, Re, In, G) \rrbracket & \text{if } G > G' \\ \llbracket (Ex', Re', In', G') \rrbracket & \text{if } G < G' \\ \llbracket (Ex \cup Ex', Re \cup Re', In \cup In', G) \rrbracket & \text{if } G = G' \end{cases}$$

where the comparison $G < G'$ is done using subterm relation, eg., $s(N) > N$. Entailment \vdash is defined as:

$$\llbracket (Ex, Re, In, G) \rrbracket \vdash (Co, Mi, e) \quad \text{iff} \quad e \in In \wedge (In \cap Co) \subseteq Ex \wedge ((In \cap Mi) \cap Re) = \emptyset.$$

Terms can be either a name m , which we will use for communications, or assertions which will be the data communicated. Assertions are a tuple of three sets of events, and a number we intend to hold the *generation* of the assertion. The first set is meant to capture what events have been executed, the second set for those events that are pending responses, and the third set for those events that are included. These three sets mimic the same sets that the marking of a DCR-graph contains. The generation number is used to get the properties of the assertion composition, which are somewhat symmetric, but still have the composition return only the latest marking/assertion (i.e., somewhat asymmetric).

The composition of two assertions keeps the assertion with highest generation.¹ This makes the composition associative, commutative, compositional, and with identity defined to be the tuple with empty sets and lowest possible generation number.

The conditions are tuples of two sets of events and a single event as the third tuple component. The first set is intended to capture the set of events that are conditions for the single event. The second set is intended to capture the set of events that are milestones for the single event.

The entailment definition mimics the definition in DCR graphs for when an event (i.e., the third component of the conditions) is enabled in a marking (i.e., the first three components of the assertions). Compare the example below with the definition of enabling from DCR graphs

$$\llbracket (Ex, Re, In, G) \rrbracket \vdash (\rightarrow \bullet e, \rightarrow \times e, e) \quad \text{iff} \quad e \in In \wedge (In \cap \rightarrow \bullet e) \subseteq Ex \wedge ((In \cap \rightarrow \times e) \cap Re) = \emptyset.$$

¹For technical reasons, when we compose two assertions with the same generation number we obtain an assertion where the sets are the union between the associated sets in each assertion, and the generation number is unchanged.

Definition 4.2 We define the function DCRPSI which takes a DCR $(E, M \rightarrow \bullet, \bullet \rightarrow, \rightarrow \diamond, \rightarrow +, \rightarrow \%, L, l)$ with distinguished marking $M = (Ex', Re', In')$ and returns a dcrPsi process

$$P_{\text{dcr}} = P_s | P_E$$

where

$$P_s = \langle (Ex', Re', In', 0) \rangle | \bar{m} \langle (Ex', Re', In', 0) \rangle. \mathbf{0} \quad \text{and} \quad P_E = |_{e \in E} P_e$$

with

$$P_e = !(\text{case } \varphi_e : \underline{m} \langle (X_E, X_R, X_I, X_G) \rangle. \\ (\bar{m} \langle (X_E \cup \{e\}, (X_R \setminus \{e\}) \cup e \bullet \rightarrow, (X_I \setminus e \rightarrow \%) \cup e \rightarrow +, s(X_G)) \rangle. \mathbf{0} | \\ ((X_E \cup \{e\}, (X_R \setminus \{e\}) \cup e \bullet \rightarrow, (X_I \setminus e \rightarrow \%) \cup e \rightarrow +, s(X_G)) \rangle))$$

where X_E, X_R, X_I, X_G are variables and $\varphi_e = (\rightarrow \bullet e, \rightarrow \diamond e, e)$.

The process P_{dcr} generated by DCRPSI contains a starting processes P_s that models the initial marking of the encoded DCR as an assertion process, and also communicates this assertion on the channel m . The rest of the process, i.e., P_E captures the actual DCR, being a parallel composition of processes P_e for each of the events of the encoded DCR. The events in a DCR can happen multiple times, hence the use of the replication operation as the outermost operator. Each event is encoded, following the ideas for event structures, using the **case** construct with a single guard φ_e . The guard contains the information for the event e that need to be checked against the current marking (i.e., the assertion) to decide if the event is enabled; these information are the set of events that are prerequisites for e (i.e., $\rightarrow \bullet e$) and the set of milestones related to e . There may be several events enabled by a marking, hence several of the parallel **case** processes may have their guards entailed by the current assertion. Only one of these input actions will communicate with the single output action on m , and will receive in the four variables the current marking. After the communication, the input process will leave behind an assertion process containing an updated marking, and also a process ready to output on m this updated marking. In fact, after a communication, what is left behind is something looking like a P_s process, but with an updated marking. The updating of the marking follows the same definition from the DCRs.

Lemma 4.3 For any DCR graph \mathcal{D} , the frame of the corresponding process $\text{DCRPSI}(\mathcal{D})$ corresponds to the marking of the encoded DCR (i.e., the first three components).

Proof: $\text{DCRPSI}(\mathcal{D})$ return a dcrPsi process with only one assertion which thus is the frame. This assertion is made directly from the marking of \mathcal{D} and added generation 0. \square

Lemma 4.4 For any DCR graph \mathcal{D} , in the execution graph of the corresponding process $\text{DCRPSI}(\mathcal{D})$ at any execution point there will be only one output process.

Proof: Initially we have only one output in the P_s part of $\text{DCRPSI}(\mathcal{D})$. Inductively we assume a reachable process P with only one output process. If we have any enabled input processes only one of these processes will join a communication with the single output process. All input processes are of the form P_e , which reduces with psi rules for replication and input to

$$P_e | (\bar{m} \langle (X_E \cup \{e\}, (X_R \setminus \{e\}) \cup \bullet \rightarrow e, (X_I \setminus e \rightarrow \%) \cup \rightarrow + e, s(X_G)) \rangle. \mathbf{0} | \\ ((X_E \cup \{e\}, (X_R \setminus \{e\}) \cup \bullet \rightarrow e, (X_I \setminus e \rightarrow \%) \cup \rightarrow + e, s(X_G)) \rangle))$$

with X_E, X_R, X_I, X_G substituted with the terms that were sent. The output process reduces to $\mathbf{0}$. We have added as many new output processes as we have removed, and as we initially only have one output process by induction we always will have only one. \square

Lemma 4.5 *For any DCR graph \mathcal{D} , in the corresponding process $\text{DCRPSI}(\mathcal{D})$ the message being sent will always be the same as the frame of the dcrPsi process.*

Proof: Initially, the first message being sent by P_s is by construction the same as the initial frame. The proof of Lemma 4.4 shows that with each communication a new assertion is added and a new sender replaces the old one. The two new terms (i.e., the assertion process and the message) are identical and have the generation part increased by one. Since the composition of assertions keeps only the assertion with the higher generation, all older assertion processes that are still present are being ignored when computing the frame of the new process. We thus have our result. \square

Lemma 4.6 (generations count transitions) *The generation part of the frame is the same as the number of transitions we have done from the initial process.*

Proof: We use induction and assume we have done n transitions and the generation part of our frame is n' where $n = n'$. From Lemma 4.5 we have that the frame and message are equal, so we will be sending n as generation part of the message. After the communication a new assertion with generation $s(n')$ is added, which by the definition of assertion composition will be the new frame. By our assumption $s(n') = s(n) = n + 1$. From Lemma 4.3 we have that $n = n' = 0$ for the initial process, and by induction we have that this holds for any number of transitions. \square

Theorem 4.7 (preserving transitions) *In a DCR graph \mathcal{D} , for any transition $(\mathcal{D}, M) \xrightarrow{e} (\mathcal{D}, M')$ there exists a reduction between the corresponding dcrPsi processes $\text{DCRPSI}(\mathcal{D}, M) \xrightarrow{\tau} \text{DCRPSI}(\mathcal{D}, M')$.*

Proof: From Lemma 4.3 we know that the frame and marking are the same. This means that since $M \vdash e$, the corresponding condition in the $\text{DCRPSI}(\mathcal{D}, M)$ will be entailed by the frame. Therefore a communication is possible, i.e., a transition labelled by τ . For $M = (Ex, Re, In)$ it means that the frame of $\text{DCRPSI}(\mathcal{D}, M)$ is (Ex, Re, In, G) . From Lemma 4.5 we know that the frame is always the same as the message being sent. When the transition corresponding to the event e happens the new frame of the dcrPsi becomes

$$((Ex \cup \{e\}, (Re \setminus \{e\}) \cup \bullet \rightarrow e, (In \setminus e \rightarrow \%) \cup e \rightarrow +, s(G)))$$

after alpha-conversion. For a transition in DCR over the event e we get the new marking

$$M' = (Ex \cup \{e\}, (Re \setminus \{e\}) \cup e \bullet \rightarrow, (In \setminus e \rightarrow \%) \cup e \rightarrow +),$$

which is the same as the new frame, with the exception of the generation part. \square

Interesting would be to look closer at the encoding of event structures through the ESPSI and the encoding through DCRPSI when seen as a special case of DCRs; a question on these lines would be: are $\text{ESPSI}(ES)$ and $\text{DCRPSI}(\text{DCR}(ES))$ bisimilar? First of all, ESPSI translates into the eventPsi instance, whereas DCRPSI into the dcrPsi instance, and these two instances work with different terms and operator definitions. Even more, the encoding of event structures exhibits behaviour through *labelled transitions*, whereas the behaviour of dcrPsi encodings exposes *only τ -transitions*. Therefore, it is not easy to find a bisimulation-like correspondence.

Nevertheless, there are clear correlations. Consider an un-labelled event structure $(E, \leq, \#)$ and its presentation as a DCR graph $(E, M, \leq, \emptyset, \emptyset, \emptyset, \# \cup id)$ with the marking $M = (\emptyset, \emptyset, E)$; and denote the associated psi-processes by $P_{ES} = \text{ESPSI}(ES)$ and $P_{DCR} = \text{DCRPSI}(\text{DCR}(ES))$. Correlate an assertion in P_{DCR} with the assertion in P_{ES} by looking only at the first set of the quadruple (having the second set of

the quadruple, which encodes responses, always empty). The conditions of P_{DCR} have the second set of milestones always empty; whereas the first set is the same as the first set of the conditions in P_{ES} . One can now check that the entailment of a condition by an assertion in P_{ES} is the same as the corresponding entailment in the P_{DCR} , when considering also the other behaviour aspects of these two processes and how they change the assertions. But we do define this investigation to a longer version of this paper.

5 Conclusions and outlook

We have encoded the true concurrency models of prime event structures and DCR graphs into corresponding instances of psi-calculi. For this we have made use of the expressive logic that psi-calculus provides to capture the causality and conflict relations of the prime event structures, as well as the relations of DCR-graphs. The computation in the concurrency models corresponds to reduction steps in the psi-processes. The more expressive model of DCR-graphs required us to make use of the communication mechanism of psi-calculi, whereas for event structures this was not needed. The data terms we sent were tuples of terms, capturing markings of DCR-graphs with a generation number attached to them.

For the encodings we also investigated some results meant to provide more confidence in their correctness. In particular, for event structures we also looked at action refinement as well as gave the syntactic restrictions that capture the psi-processes that exactly correspond to event structures. Besides providing correlations between the computations in the respective models, we also investigated how true concurrency is correlated to the interleaving diamonds in the encodings we gave.

The purpose of our investigations was to see how well the expressiveness of psi-calculi can accommodate the expressiveness of true concurrency models. Nevertheless, a discrepancy remains between the interleaving semantics based on SOS rules of psi-calculi, and the true concurrency nature of the two models we considered. Further investigations would look for a true concurrency semantics for psi-calculi (with initial results presented as [18]), and then see how our encodings fit with the true concurrency models that this semantics would return. One could also look into adding responses to psi-calculus, similar to how is done in [5] for Transition Systems with Responses.

References

- [1] Martín Abadi & Cédric Fournet (2001): *Mobile values, new names, and secure communication*. In: *POPL*, ACM, pp. 104–115. Available at <http://doi.acm.org/10.1145/360204.360213>.
- [2] Martín Abadi & Andrew D. Gordon (1999): *A Calculus for Cryptographic Protocols: The spi Calculus*. *Inf. Comput.* 148(1), pp. 1–70. Available at <http://dx.doi.org/10.1006/inco.1998.2740>.
- [3] Jesper Bengtson, Magnus Johansson, Joachim Parrow & Björn Victor (2011): *Psi-calculi: a framework for mobile processes with nominal data and logic*. *Logical Methods in Computer Science* 7(1). Available at [http://dx.doi.org/10.2168/LMCS-7\(1:11\)2011](http://dx.doi.org/10.2168/LMCS-7(1:11)2011).
- [4] Maria Grazia Buscemi & Ugo Montanari (2007): *CC-Pi: A Constraint-Based Language for Specifying Service Level Agreements*. In: *ESOP’07, LNCS 4421*, Springer, pp. 18–32. Available at http://dx.doi.org/10.1007/978-3-540-71316-6_3.
- [5] Marco Carbone, Thomas T. Hildebrandt, Gian Perrone & Andrzej Wasowski (2012): *Refinement for Transition Systems with Responses*. In: *4th Workshop on Foundations of Interface Technologies (FIT’12), EPTCS 87*, pp. 48–55. Available at <http://dx.doi.org/10.4204/EPTCS.87.5>.
- [6] Rocco De Nicola, Gian Luigi Ferrari, Ugo Montanari, Rosario Pugliese & Emilio Tuosto (2005): *A Process Calculus for QoS-Aware Applications*. In: *COORDINATION, LNCS 3454*, Springer, pp. 33–48. Available at http://dx.doi.org/10.1007/11417019_3.

- [7] Rob van Glabbeek (2006): *On the Expressiveness of Higher Dimensional Automata*. *Theor. Comput. Sci.* 356(3), pp. 265–290. Available at <http://dx.doi.org/10.1016/j.tcs.2006.02.012>.
- [8] Rob van Glabbeek & Ursula Goltz (2001): *Refinement of actions and equivalence notions for concurrent systems*. *Acta Informatica* 37(4/5), pp. 229–327, doi:10.1007/s002360000041. Available at <http://link.springer.de/link/service/journals/00236/bibs/1037004/10370229.htm>.
- [9] Rob van Glabbeek & Gordon Plotkin (2009): *Configuration structures, event structures and Petri nets*. *Theor. Comput. Sci.* 410(41), pp. 4111–4159. Available at <http://dx.doi.org/10.1016/j.tcs.2009.06.014>.
- [10] Vincent Gupta (1994): *Chu Spaces: A Model of Concurrency*. Ph.D. thesis, Stanford University.
- [11] Thomas T. Hildebrandt & Raghava Rao Mukkamala (2010): *Declarative Event-Based Workflow as Distributed Dynamic Condition Response Graphs*. In: *PLACES, EPTCS 69*, pp. 59–73. Available at <http://dx.doi.org/10.4204/EPTCS.69.5>.
- [12] Thomas T. Hildebrandt, Raghava Rao Mukkamala & Tijs Slaats (2012): *Nested Dynamic Condition Response Graphs*. In: *4th IPM International Conference on Fundamentals of Software Engineering (FSEN), LNCS 7141*, Springer, pp. 343–350. Available at http://dx.doi.org/10.1007/978-3-642-29320-7_23.
- [13] Hans Hüttel (2011): *Typed psi-calculi*. In Joost-Pieter Katoen & Barbara König, editors: *22nd International Conference on Concurrency Theory (CONCUR'11), LNCS 6901*, Springer, pp. 265–279. Available at http://dx.doi.org/10.1007/978-3-642-23217-6_18.
- [14] Hans Hüttel (2013): *On Representing Located Process Calculi in the psi-calculus*. personal communication.
- [15] Robin Milner (1983): *Calculi for Synchrony and Asynchrony*. *Theor. Comput. Sci.* 25, pp. 267–310, doi:10.1016/0304-3975(83)90114-7.
- [16] Robin Milner, Joachim Parrow & David Walker (1992): *A Calculus of Mobile Processes, I-II*. *Information and Computation* 100(1), pp. 1–77, doi:10.1016/0890-5401(92)90008-4.
- [17] Mogens Nielsen, Gordon Plotkin & Glynn Winskel (1979): *Petri Nets, Event Structures and Domains*. In: *Semantics of Concurrent Computation, LNCS 70*, Springer, pp. 266–284, doi:10.1007/BFb0022474.
- [18] Håkon Normann, Cristian Prisacariu & Thomas Hildebrandt (2014): *True Concurrency Semantics for Psi-calculi*. In: *1st International Workshop on Meta Models for Process Languages (MeMo)*. (presentation).
- [19] Andrew M. Pitts (2013): *Nominal Sets: Names and Symmetry in Computer Science*. *Cambridge Tracts in Theoretical Computer Science* 57, Cambridge Univ. Press, doi:10.1017/CB09781139084673.
- [20] Vaughan R. Pratt (1991): *Modeling Concurrency with Geometry*. In: *POPL'91*, pp. 311–322. Available at <http://doi.acm.org/10.1145/99583.99625>.
- [21] Vaughan R. Pratt (1995): *Chu Spaces and their Interpretation as Concurrent Objects*. In: *Computer Science Today: Recent Trends and Develop.*, LNCS 1000, Springer, pp. 392–405. Available at <http://dx.doi.org/10.1007/BFb0015256>.
- [22] Vaughan R. Pratt (2000): *Higher dimensional automata revisited*. *Math. Struct. Comput. Sci.* 10(4), pp. 525–548, doi:10.1017/S0960129500003169.
- [23] Tijs Slaats, Raghava Rao Mukkamala, Thomas T. Hildebrandt & Morten Marquard (2013): *Exformatics Declarative Case Management Workflows as DCR Graphs*. In: *Business Process Management, LNCS 8094*, Springer, pp. 339–354. Available at http://dx.doi.org/10.1007/978-3-642-40176-3_28.
- [24] Glynn Winskel (1982): *Event Structure Semantics for CCS and Related Languages*. In: *ICALP, LNCS 140*, Springer, pp. 561–576. Available at <http://dx.doi.org/10.1007/BFb0012800>.
- [25] Glynn Winskel (1986): *Event Structures*. In: *Advances in Petri Nets, LNCS 255*, Springer, pp. 325–392. Available at http://dx.doi.org/10.1007/3-540-17906-2_31.
- [26] Glynn Winskel & Mogens Nielsen (1995): *Models for Concurrency*. In Samson Abramski, Dov M. Gabbay & Tom S.E. Maibaum, editors: *Handbook of Logic in Computer Science – vol 4 – Semantic Modelling*, Oxford University Press, pp. 1–148.